E-ISSN: 2583-9667
Indexed Journal
Peer Reviewed Journal
https://multiresearchjournal.theviews.in

Received: 05-07-2023
Accepted: 11-09-2023

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH IN MULTIDISCIPLINARY

Volume 1; Issue 2; 2023; Page No. 560-564

Evaluating role-based access control (RBAC) for protecting electronic health records in modern healthcare

[1]Taduri Suneetha and [2]Dr. Amit Singhal

[1]Research Scholar, Department of Computer Science & Engineering, Monad University, Hapur, Uttar Pradesh, India
[2]Professor, Department of Computer Science & Engineering, Monad University, Hapur, Uttar Pradesh, India

Corresponding Author: Taduri Suneetha

Abstract

Role-Based Access Control (RBAC) has become a core component in securing electronic health records (EHRs) by assigning access rights to users based on their job roles. This study investigates the effectiveness of RBAC in healthcare, evaluating its strengths and weaknesses through a mixed-methods approach that includes a systematic literature review, surveys, and interviews with healthcare IT professionals. Analysis of survey data and organisational documents reveals that while RBAC offers a clear structure and supports regulatory compliance, challenges such as role explosion, dynamic role needs, and integration issues with modern technologies persist. The paper recommends strategies such as dynamic role assignment, regular role audits, and improved training to enhance RBAC systems. The findings provide practical insights for healthcare administrators aiming to secure patient data and improve overall data governance.

Keywords: Role-based access control, electronic health records, healthcare security, access management, data protection, RBAC, IT governance

Introduction

The digitalisation of healthcare has transformed the way patient data is stored and accessed. Electronic Health Records (EHRs) have become vital in improving patient care, yet they also pose significant challenges in terms of data security. As the volume and sensitivity of data increase, healthcare organisations must implement robust security measures to prevent unauthorised access and data breaches. One widely adopted method is Role-Based Access Control (RBAC), which ties access privileges to user roles rather than individual identities. This approach not only simplifies the management of permissions in large organisations but also helps ensure that users access only the data necessary for their roles.

Despite its popularity, the practical implementation of RBAC in healthcare is not without challenges. Dynamic environments, such as hospitals, experience frequent staff rotations, overlapping responsibilities, and emergency scenarios that demand flexible access controls. Furthermore, as healthcare technology rapidly evolves-with telemedicine, mobile health applications, and cloud computing becoming prevalent-traditional RBAC systems may struggle to adapt without additional support measures.

This paper aims to critically evaluate the effectiveness of RBAC for protecting EHRs within modern healthcare settings. By drawing on a comprehensive literature review, surveys, and interviews with IT professionals and healthcare administrators, the study seeks to:

- Examine the theoretical foundations and current applications of RBAC.
- Identify practical challenges and limitations in real-world implementations.
- Propose recommendations for refining RBAC systems to better accommodate dynamic healthcare environments.

The following sections detail the literature review, methodology, results, discussion, and conclusions drawn from the research.

Literature Review

The literature on RBAC spans both theoretical frameworks and practical applications. Early work on RBAC laid the foundation by introducing the concept of assigning permissions to roles rather than individuals (Ferraiolo *et al*., 1995; Sandhu *et al*., 1996) [6, 21]. This model simplifies access management and has been widely adopted in sectors where data security is paramount, including healthcare.

Theoretical Foundations of RBAC

RBAC is built on the principle that users are assigned to roles corresponding to their job functions. Each role is granted specific permissions, and users inherit these permissions when they are assigned the role. This model improves administrative efficiency and enhances security by limiting access to only what is necessary for a particular function (Thomas & Sandhu, 1997) [23]. The separation of duties is a critical security principle that RBAC supports by preventing a single user from having conflicting privileges.

RBAC in Healthcare

In healthcare, the use of RBAC is particularly relevant given the diverse roles within clinical settings. Physicians, nurses, administrative staff, and support personnel require varying degrees of access to patient data. The granular control offered by RBAC allows institutions to limit access based on the necessity of each role. Studies have shown that organisations with well-implemented RBAC systems tend to have fewer unauthorised access incidents and better compliance with regulatory frameworks such as HIPAA and GDPR (Kraemer & Carayon, 2017; Alotaibi & Federico, 2017) [11, 2].

Table 1: Key Components of RBAC in Healthcare

Component	Description
Role Definition	Clear delineation of responsibilities (e.g., physician, nurse, admin staff)
Permission Assignment	Mapping of specific access rights to each role
User Assignment	Process of assigning healthcare professionals to defined roles
Audit Trails	Logging user activity to monitor compliance and detect breaches

Advantages of RBAC

Numerous studies highlight the benefits of RBAC:

- **Administrative Efficiency:** RBAC reduces the overhead associated with managing individual permissions, especially in large institutions (Cram *et al*., 2016) [4].
- **Regulatory Compliance:** Clear audit trails and predefined roles support adherence to legal and regulatory standards (Wiederhold *et al*., 2019) [24].
- **Scalability:** As healthcare organisations grow, RBAC can scale to include new roles without overhauling the entire access control system (Alhaqbani & Fidge, 2008) [1].

Challenges and Limitations

Despite its strengths, RBAC is not without limitations:

- **Role Explosion:** The proliferation of overly specific roles can lead to administrative complexity and inefficiency (Lai *et al*., 2019) [13].
- **Dynamic Role Requirements:** Healthcare environments often require flexible access control during emergencies or temporary role changes (Ni *et al*., 2021) [17].
- **Integration Issues:** New technologies such as telemedicine and mobile health platforms sometimes operate on different access control models, complicating integration with existing RBAC systems (Kuo *et al*., 2017) [12].

Table 2: Challenges in Implementing RBAC

Challenge	Impact on Healthcare
Role Explosion	Increases complexity; may lead to redundant or conflicting roles
Dynamic Role Requirements	Difficulty in adapting to temporary or emergency access needs
Integration with New Tech	Compatibility issues with telemedicine and mobile health applications
Organisational Resistance	Lack of training and support may result in poor adherence to RBAC policies

Research Gaps

Although the literature acknowledges RBAC's potential benefits, empirical studies on its real-world performance in dynamic healthcare environments are limited. Additionally, few studies have addressed how emerging technologies can be seamlessly integrated into existing RBAC frameworks, signalling a need for further research in this area.

Materials and Methods

This study adopted a mixed-methods approach to evaluate the implementation and efficacy of RBAC in protecting EHRs within healthcare organisations.

Research Design

A combination of qualitative and quantitative methods was used:

- **Systematic Literature Review:** Academic databases such as PubMed, IEEE Xplore, and ScienceDirect were searched using keywords like "RBAC," "Electronic Health Records," and "Healthcare Security."
- **Surveys:** An online survey was distributed to 120 healthcare IT professionals across various institutions in the UK. The questionnaire featured Likert-scale questions and open-ended responses regarding RBAC implementation and challenges.
- **Semi-Structured Interviews:** In-depth interviews were conducted with 15 healthcare administrators and IT security experts. These interviews aimed to explore practical challenges and gather case-specific insights.
- **Document Analysis:** Policy documents and access logs from two major hospitals were reviewed to compare theoretical RBAC frameworks with actual practices.

Data Collection

- **Surveys:** The survey was administered over a period of four weeks, achieving a response rate of 65% (78 completed responses). Participants were selected through convenience and snowball sampling.
- **Interviews:** Interviews were conducted either face-to-face or via secure video conferencing. Each interview lasted approximately 30–40 minutes and was recorded and transcribed with participant consent.
- **Document Analysis:** Access logs and RBAC policy documents were collected in digital format. These documents were anonymised and analysed for consistency with survey and interview findings.

Data Analysis

- **Quantitative Data:** Survey responses were analysed using descriptive statistics and chi-square tests in SPSS. Data visualisations, including frequency tables and

charts, were produced to highlight key trends.
- **Qualitative Data:** Interview transcripts were coded using thematic analysis to identify recurring themes and patterns. NVivo software supported the coding process, ensuring that themes were consistently categorised.
- **Triangulation:** Data from surveys, interviews, and document analysis were cross-checked to enhance the reliability of the findings.

Ethical Considerations

Ethical approval was obtained from the relevant institutional review boards. All participants were informed of the study's purpose and provided consent prior to participation. Confidentiality was maintained through anonymisation of data, and access to raw data was restricted to the research team.

Results

The study's findings are based on data collected from 78 survey respondents, 15 in-depth interviews, and the analysis of policy documents and access logs from two hospitals.

Survey Findings

- **Adoption of RBAC:** 85% of respondents indicated that their organisation had implemented an RBAC system.
- **Effectiveness:** 70% agreed or strongly agreed that RBAC was effective in preventing unauthorised access, while 18% were neutral, and 12% disagreed.
- **Administrative Challenges:** 60% found the management of RBAC moderately challenging to very challenging, citing issues such as role explosion and infrequent role updates.
- **Training:** Only 40% of respondents reported receiving regular training on RBAC policies.

Table 3: Survey Responses on RBAC Adoption and Challenges

Survey Item	Percentage (%)
Organisations using RBAC	85
Perceived effectiveness of RBAC	70 (agree/strongly agree)
Reporting administrative challenges	60
Regular training provided	40

Interview Insights

The interviews reinforced the survey findings. Key themes included:

- **Role Clarity:** Most interviewees stressed the need for clear, regularly updated role definitions.
- **Emergency Access:** Respondents expressed concerns about the rigidity of RBAC during emergencies, suggesting the need for well-monitored "break-glass" protocols.
- **Cultural and Training Issues:** A recurring concern was the lack of continuous training and the impact of organisational culture on the effective implementation of RBAC.

Document Analysis

The analysis of hospital documents revealed that:

- One hospital maintained comprehensive RBAC policies with regular audits, whereas the other had outdated documentation leading to inconsistencies.
- Access logs frequently showed "role creep," where staff retained permissions from previous roles even after changing positions.

Table 4: Summary of Document Analysis

Hospital	RBAC Policy Status	Key Findings
Hospital A	Comprehensive and regularly audited	Minimal role creep; clear role definitions
Hospital B	Outdated documentation	Significant role creep; inconsistencies in permissions

Findings and Discussion

The data collected from surveys, interviews, and document reviews offer a comprehensive view of RBAC implementation in healthcare settings.

Effectiveness of RBAC

The high rate of RBAC adoption (85%) suggests that healthcare organisations recognise the model's potential to streamline access management and protect sensitive patient data. However, the 70% positive response on effectiveness is tempered by the fact that a significant proportion of respondents (30%) remained neutral or negative. This indicates that while RBAC is valued, its implementation is not without shortcomings.

The Role of Clear Role Definitions

The importance of clear role definitions emerged as a central theme. Organisations that invest in detailed role mapping and regular updates tend to experience fewer security lapses. As demonstrated by Hospital A's practices, regular audits and clear policies can minimise "role creep" and ensure that access privileges remain appropriate. In contrast, outdated policies-as seen in Hospital B-can lead to inefficiencies and potential security risks.

Administrative Challenges and Training

The administrative burden of managing RBAC was highlighted by 60% of survey respondents. Complex role hierarchies and the creation of niche roles (role explosion) contribute significantly to these challenges. Regular training is essential to ensure that staff understand their responsibilities and adhere to the protocols. The relatively low percentage (40%) of respondents receiving regular training points to an area where many organisations can improve.

Organisational Culture and Emergency Access

Interview data emphasised that organisational culture plays a pivotal role in RBAC's success. Institutions that foster a strong security culture and provide continuous training are more likely to implement RBAC effectively. Additionally, several interviewees raised concerns about the rigidity of RBAC in emergency situations. In these cases, break-glass policies are often implemented; however, these measures require strict monitoring and clear guidelines to prevent misuse while still ensuring that patient care is not compromised.

Integration with Emerging Technologies

Healthcare is undergoing rapid technological change. The integration of telemedicine and mobile health applications introduces new challenges for RBAC systems. Many

organisations struggle to reconcile traditional RBAC with the dynamic access needs imposed by these technologies. This study suggests that hybrid models, incorporating elements of Attribute-Based Access Control (ABAC) or context-aware systems, could provide the necessary flexibility while retaining the benefits of RBAC.

Comparative Analysis

To further illustrate the challenges and strengths of RBAC, consider the following comparative insights from the study:

- **Organisations with Regular Audits:** Show a lower incidence of unauthorised access and role creep.
- **Organisations Without Regular Training:** Exhibit a higher frequency of access errors and inefficiencies in role management.
- **Dynamic Role Environments:** Face difficulties in maintaining up-to-date role definitions, underscoring the need for automated or dynamic role assignment tools.

Table 5: Comparative Overview of Organisations

Organisation Feature	High-Performing RBAC	Low-Performing RBAC
Regular Audits	Yes	No
Staff Training Frequency	Frequent	Infrequent
Policy Update Frequency	Regular (Quarterly)	Irregular/Outdated
Adaptability to Emergencies	Well-defined break-glass protocols	Rigid access controls

Recommendations

Based on the findings, the following recommendations are proposed to enhance RBAC systems in healthcare:

1. **Dynamic Role Assignment:** Incorporate real-time context into role management. Temporary elevation of access rights during emergencies, followed by automatic reversion, can help balance security with clinical needs.
2. **Regular Audits and Policy Reviews:** Organisations should conduct periodic audits and update RBAC policies to prevent role creep and ensure that access permissions align with current organisational structures.
3. **Comprehensive Training Programs:** Establish mandatory, continuous training programmes for all staff to ensure understanding and adherence to RBAC policies.
4. **Enhanced Integration Frameworks:** Develop standardised protocols for integrating RBAC with emerging technologies such as telemedicine platforms and mobile health applications.
5. **Robust Break-Glass Mechanisms:** Implement and monitor break-glass protocols rigorously, ensuring that any temporary access overrides are logged and reviewed.

These recommendations are intended to support healthcare organisations in refining their access control frameworks, thereby enhancing patient data protection while accommodating the demands of a dynamic healthcare environment.

Conclusion

This research has evaluated the role of RBAC in protecting electronic health records within modern healthcare settings. The findings indicate that while RBAC is widely adopted and generally effective, its success depends heavily on clear role definitions, regular training, and continuous policy audits. Organisations with robust RBAC practices demonstrate improved security and regulatory compliance, yet many still struggle with issues such as role explosion, dynamic access needs, and integration challenges with new technologies.

The study recommends adopting dynamic role assignment, conducting regular audits, and improving staff training to mitigate these challenges. Future research should explore hybrid access control models that combine RBAC with context-aware or attribute-based methods to further enhance flexibility and security. In an era where the digitisation of healthcare continues to accelerate, optimising RBAC remains crucial for safeguarding patient data and maintaining public trust.

References

1. Alhaqbani B, Fidge C. Access control requirements for processing electronic health records. AusGrid Conference Proceedings; c2008. p. 23–32.
2. Alotaibi YK, Federico F. The impact of health information technology on patient safety. Saudi Medical Journal. 2017;38(12):1173-1180.
3. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77–101.
4. Cram WA, Proudfoot JG, D'Arcy J. Organisational information security policies: a review and research framework. European Journal of Information Systems. 2016;25(6):605-641.
5. Eze E, Gleasure R, Heavin C. Exploiting the digital patient experience: a critical analysis of telehealth. Information Systems Frontiers. 2020;22(2):247-266.
6. Ferraiolo DF, Kuhn R, Chandramouli R. Role-based access control (RBAC): Features and motivations. CSA Conference Proceedings; c1995. p. 241-248.
7. Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, *et al*. Guide to Attribute-Based Access Control (ABAC). NIST Special Publication; c2012. 800-862.
8. Hu VC, Kuhn R, Ferraiolo DF. Attribute-based access control. Computer. 2015;48(2):85-88.
9. Johnson ME, Stoudemire S, Gofman M. Comparing role-based and attribute-based access control in healthcare. Journal of Information Privacy and Security. 2018;14(1):3-18.
10. Johnson C, Jones A. The evolution of healthcare data security in the digital era. Health Informatics Journal. 2020;26(3):1612-1625.
11. Kraemer S, Carayon P. Cybersecurity in healthcare: modern threats and trends. Technology and Health Care. 2017;25(6):1-10.
12. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. JAMIA. 2017;24(6):1211-1220.

13. Lai AM, Ramesh A, Mahan M, Chokshi SK. Improving health IT implementation: a qualitative study. BMJ Open. 2019;9(9):e030528.
14. Lee H, Park E, Kim J. Healthcare data breach trends and implications for security policies. Journal of Medical Internet Research. 2022;24(4):e30834.
15. Martin KE, Nissenbaum H. Privacy interests in public records: an empirical investigation. Harvard Journal of Law & Technology. 2017;31(1):111-167.
16. Miller T, Roberts A. Telemedicine expansion and RBAC implications: a survey of US hospitals. Telemedicine and e-Health. 2022;28(7):977-984.
17. Ni Q, Lin D, Bertino E. Privacy-aware role-based access control. ACM TISSEC. 2021;24(3):16.
18. NIST. Security and Privacy Controls for Information Systems. NIST SP 800-53 Rev. 5; 2020.
19. Office for National Statistics. Cyber Security Breaches Survey. UK Government; c2021.
20. Park J, Park Y. Comparative analysis of RBAC and ABAC in cloud-based EHR systems. Computers & Security. 2023;123:102959.
21. Sandhu R, Coyne E, Feinstein H, Youman C. Role-based access control models. Computer. 1996;29(2):38–47.
22. Smith G, Johnson D. Enhancing RBAC with dynamic contextual rules in emergency medicine. Journal of Healthcare Engineering. 2021;2021:8812539.
23. Thomas R, Sandhu R. Task-based authorization controls (TBAC) for enterprise systems. Springer; c1997. p. 166-181.
24. Wiederhold G, Gupta A, Memon N. Cybersecurity challenges in healthcare: regulatory perspectives. Health Affairs. 2019;38(11):1840-1847.
25. Zhang L, Yu H, Chen D. Context-aware access control for patient monitoring in smart homes. Sensors. 2019;19(2):276.
26. Brown T, O'Sullivan M, Anderson P. Evaluating RBAC in hospital data protection: a multi-case study. International Journal of Medical Informatics. 2021;152:104479.
27. Kulkarni S, Smith A, Martin T. AI-enhanced healthcare data security. BMC Med Inform Decis Mak. 2020;20(1):278.
28. Eze E, Gleasure R, Heavin C. Telehealth and security: challenges in modern healthcare. Inf. Syst. Frontiers. 2020;22(2):247-266.
29. ISO/IEC. ISO/IEC 27002:2022 Information Security Controls. International Organization for Standardization; c2022.
30. NHS Digital. Data Security and Protection Toolkit Guidance. Department of Health and Social Care; c2023.